[0115] This embodiment of a color determination routine therefore provides for rapid determination of color authenticity for each composite color pixel **1110**. Accordingly, the user may be notified whether the color of a pixel **1110** is associated with an authentic pigment color (inside the color cone **700**), or with a copy of an authentic pigment color (outside the color cone **700**).

[0116] Further, in reference to **FIG. 12**, it can be noted that the valid color areas do not actually intersect with the point of origin in the color space. This is because, in practice, colors may not be "pure" or precisely matched to the device **5** (i.e., the color of the security features may be at least somewhat mismatched with the color filters **22** of the lens/CCD system **20**). However, displacement of a valid color area **8705**, **8706** from the point of origin in the color space need not perturb the ability to accept or reject a color as described herein. One method to improve the relationship of a valid color area **8705**, **8706** in relation to the point of origin, is through calibration of the device **5**.

[0117] A number of factors can affect how well a device **5** will detect security features within a document. For example, CCD sensitivity and illumination conditions can play a significant role in authenticity determinations. In preferred embodiments, a process called "training," or "calibration" of the device **5** is completed prior to making authenticity determinations. Training is completed in order to reduce variability between readers **5**, improve detection of security features, and to improve counterfeit rejection.

[0118] In one embodiment of a training sequence, each device **5** creates its own color cones **700**. In order to train a reader **5**, a document standard is placed into conditions that will be typical of measurement conditions. That is, the lighting, sensor **20** to target **200** geometry, and other considerations, are as close as possible to operational conditions. One example of a document standard **1210** is shown in **FIG. 15**. In one embodiment, the document standard **1210** is produced by obtaining an authentic version the substrate (which includes a distribution of security features **1150**), when the substrate is newly produced or freshly minted. In other embodiments, the document standard **1210** is taken from a population of worn authentic substrate **200**. Multiple standards **1210** may be used, in any appropriate combination of conditions.

[0119] Aspects of the document standard **1210** are programmed or downloaded into the device **5**. The device **5** then acquires and analyzes at least one image **404** of the standard **1210**. The device **5** then generates a variety of calibration coefficients which relate image data to the standard **1210**. For example, a device **5** may generate its own color cone information. In other embodiments, the device **5** may generate calibration coefficients that relate image data to authentic size ranges for the security features. In further embodiments, the device **5** may generate calibration coefficients upon completion of an appropriate series of measurements of one or more standards **1210**. In these embodiments, the device **5** may further develop calibration coefficients based upon a statistical analysis of device **5** performance characteristics. Further training routines may involve, without limitation, the use of close counterfeit documents **200**, and the subsequent analysis of false-positive performance data. Training of the device **5** may be completed through automated and/or manual techniques.

[0120] Once a pixel block **1110** has been found that is a valid color for a security particle **1150**, the CMS **15**A may determine other aspects as appropriate. For example, the CMS **15**A may determine geometric aspects, or morphological aspects, of a security feature such as, and not limited to, the shape or size of the candidate particle **1150** producing the valid color. For convenience, such determinations are referred to as "shape determinations" although these aspects are not limited to a shape or size. For example, morphological aspects may include a study of the structure or form of the candidate particle **1150**. This may include analysis of the shape and structure of the candidate particle **1150**, as distinguished from the material forming the particle **1150**. More specifically, such an analysis may consider the thickening of the particle **1150** (from one portion of the particle in relation to another), a thinning of the particle **1150**, connected components (which particles **1150** overlap), and other similar analyses.

[0121] In one embodiment of a shape determining algorithm, the CMS **15**A searches for the left edge of the particle **1150**, using gray level thresholds. Once the left edge has been found, the CMS **15**A proceeds in a clockwise direction to trace the perimeter of the candidate particle **1150** while counting the number of pixel blocks **1110** traversed. In this exemplary embodiment, if the number of pixel blocks **1110** exceeds a fixed limit, the candidate particle **1150** is rejected. For example, valid security particles **1150** may be considered to have perimeters that range in pixel **1110** counts from six to ten pixels **1110** for a given color. For example, if the CMS **15**A encounters a particle **1150** having a valid color, the CMS **15**A will trace the perimeter of the candidate particle **1150** by counting contiguous pixels **1110** where an outer edge of the particle **1150** appears. The CMS **15**A will total the number of contiguous pixels **1110**. If the total count is a number outside of the acceptable range, the particle **1150** is rejected. In this example, particles **1150** that fall within the range of six to ten pixels **1110** are accepted as valid security particles **1150**, and counted as an occurrence of acceptable size comparison information. In the embodiment depicted in **FIG. 10A**, each of the security particles **1150** fall within the range of acceptability, and therefore pass the size comparison test, also referred to as a "perimeter walk test." Such evaluations may therefore be referred to as "doing a perimeter walk," or "performing a perimeter walk." The "perimeter walk" algorithm is particularly useful for small circularly symmetric objects, but other techniques for more complex shapes may be used. For example, connected components analysis, thinning and thickening analyses, and hit-or-miss transforms are among the other morphology determining algorithms that may be employed.

[0122] As an example, consider a hit-or-miss transform. Generally, the hit-or-miss transform is a template matching. Consider a black and white image containing thee different sizes of white squares on a black background. The transform is employed as a search technique to find the middle sized square. A template is laid over the image, and used to scan for the exact shape you trying to match, which is the middle size square. Preferably, the template contains a feature sized to match the target portion of the image (middle sized square). When the template feature is completely white, data is entered into a reference index to make a record of that location. As one example, a copy of the image is marked with a dot for each of the middle sized squares. Both the smaller and the larger squares are not entered into the record.